Combat IT Sabotage: Technical Solutions From The CERT Insider Threat Lab

Dawn Cappelli

Joji Montelibano

Software Engineering Institute -

CERT Insider Threat Center

Session ID: HT2-108

Session Classification: Intermediate

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
FEB 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Combat IT Sabotage: Technical Solutions From The CERT Insider Threat Lab	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Carnegie Mellon University,Software Engineering Institute,Pittsburgh,PA,15213**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
RSA Conference 2011, held in San Francisco, CA from February 14-18, 2011.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**28**	

Notices

Demonstration: Malicious Modification of Source Code

Agenda

- Background
- Crime Profile: Insider IT Sabotage
- Countermeasures: Insider IT Sabotage
- Wrap-Up / Discussion

What is CERT?

- Center of Internet security expertise
- Established in 1988 by the US Department of Defense on the heels of the Morris worm that created havoc on the ARPANET, the precursor to what is the Internet today
- Located in the Software Engineering Institute (SEI)
  - Federally Funded Research & Development Center (FFRDC)
  - Operated by Carnegie Mellon University (Pittsburgh, Pennsylvania)

Who is a Malicious Insider?

Current or former employee, contractor, or other business partner who

- *has or had authorized access to an organization's network, system or data and*
- *intentionally exceeded or misused that access in a manner that*
- *negatively affected the confidentiality, integrity, or availability of the organization's information or information systems.*

CERT Insider Threat Center

- A decade of experience in the insider threat area
- Sponsors / partners include:
  - US Secret Service
  - Department of Homeland Security
  - Carnegie Mellon CyLab
  - DoD Personnel Security Research Center
  - DoD and Counterintelligence
  - Office of the National Counterintelligence Executive
  - Air Force Research Laboratory
  - Defense Industrial Base members
  - Other federal agencies

Mission of the CERT Insider Threat Center

Improve the preparedness level of the community to prevent, detect, and respond to insider crimes

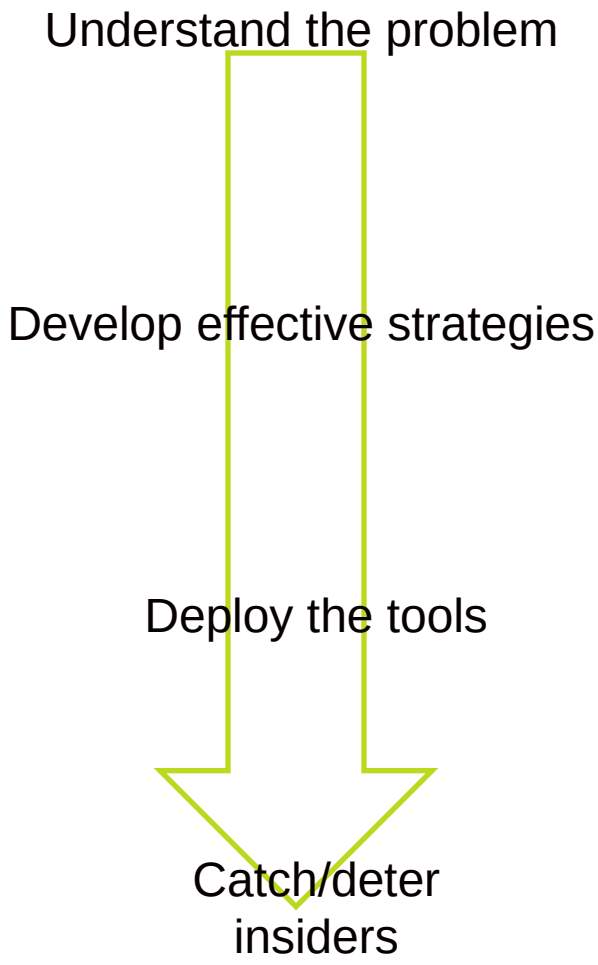
Desired impact:

- Organizations will have
  - A more accurate understanding of the lifecycle of insider threats
  - Improved defenses against the types of compromises seen in actual cases
  - Reduction in the number and impact of insider incidents
- National security should improve as a result

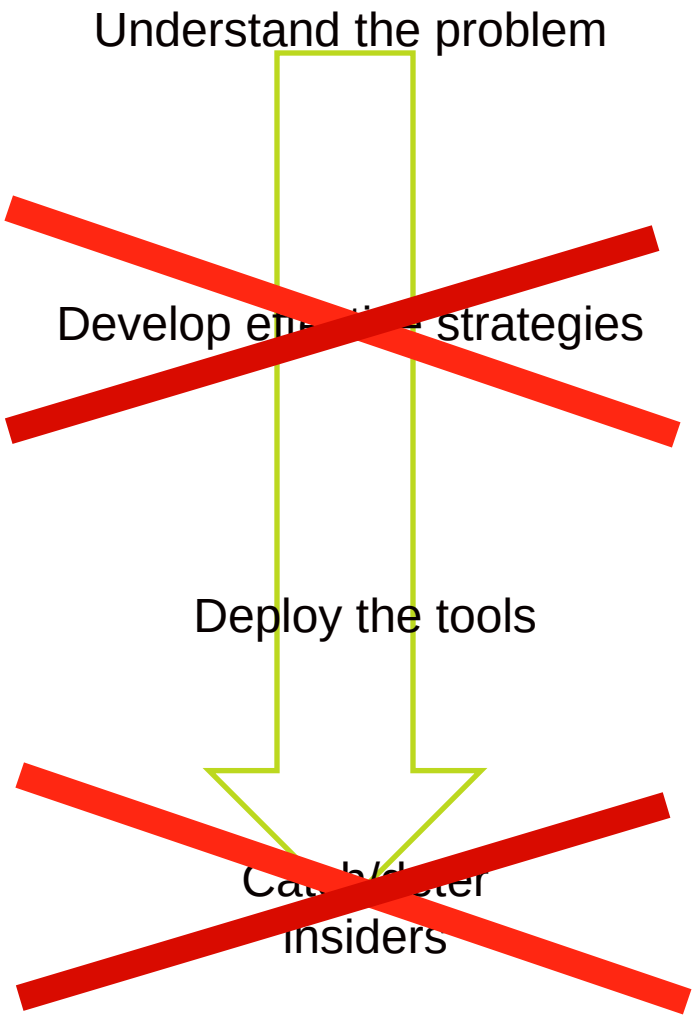
CERT Insider Threat Center Goals

- Identify policies, procedures, and technologies that can mitigate the risk of insider threat
- Develop and validate new and existing insider threat controls (including improved automated sensors)
- Transition controls and influence standards

Desired State



Current State



Current Body of Work

Cases
Assessments
Metrics
Lit Reviews

Controls

Open source solutions

Optimized configurations for commercial technology

Risk scoring algorithms

New functional requirements

Insider threat risk management process

Workshops

Senior Executive Workshops

Demos

VTE Modules

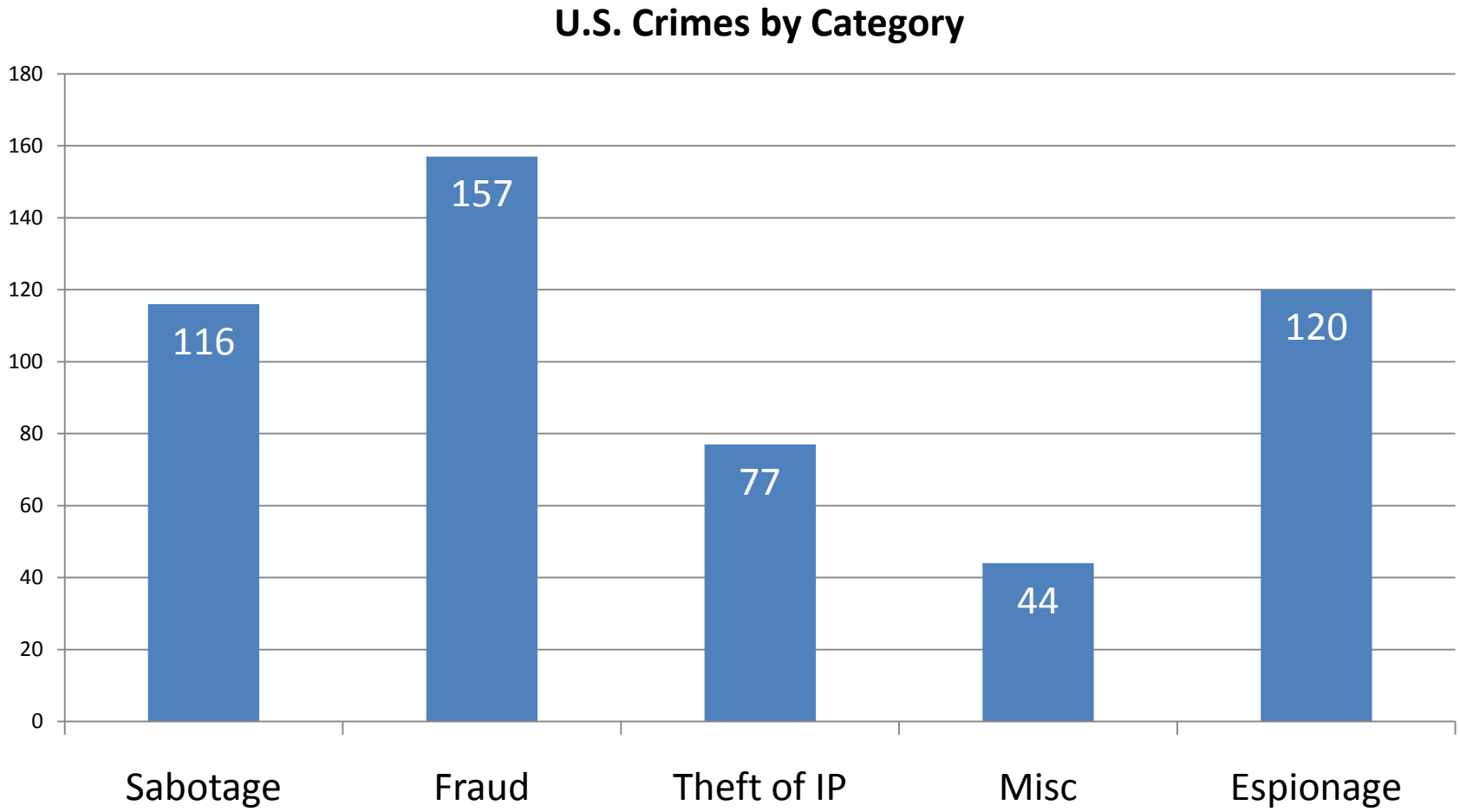
Exercises

Incident Response

Forensic Investigations (internal & external attacks)

Standards

CERT's Insider Threat Case Database



This Presentation

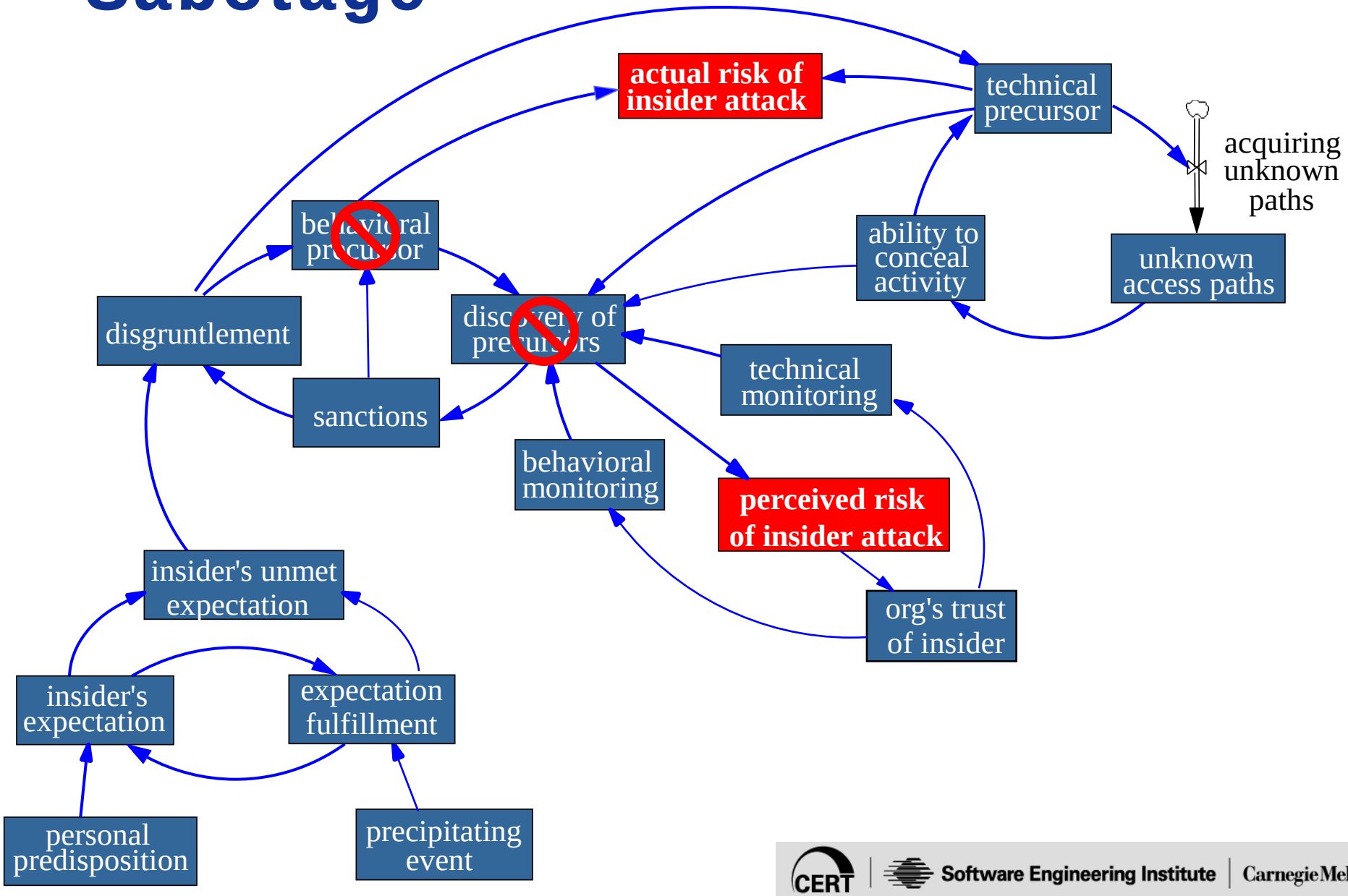
- Starts with a quick overview of CERT's crime profile for insider IT sabotage
- Follows with demonstrations based on actual case examples to present potential countermeasures
- Then you can compare your defensive strategies to our controls, and determine whether your existing controls are sufficient to prevent and detect insider attacks such as those shown in the case studies.

Crime Profile:
Insider IT Sabotage

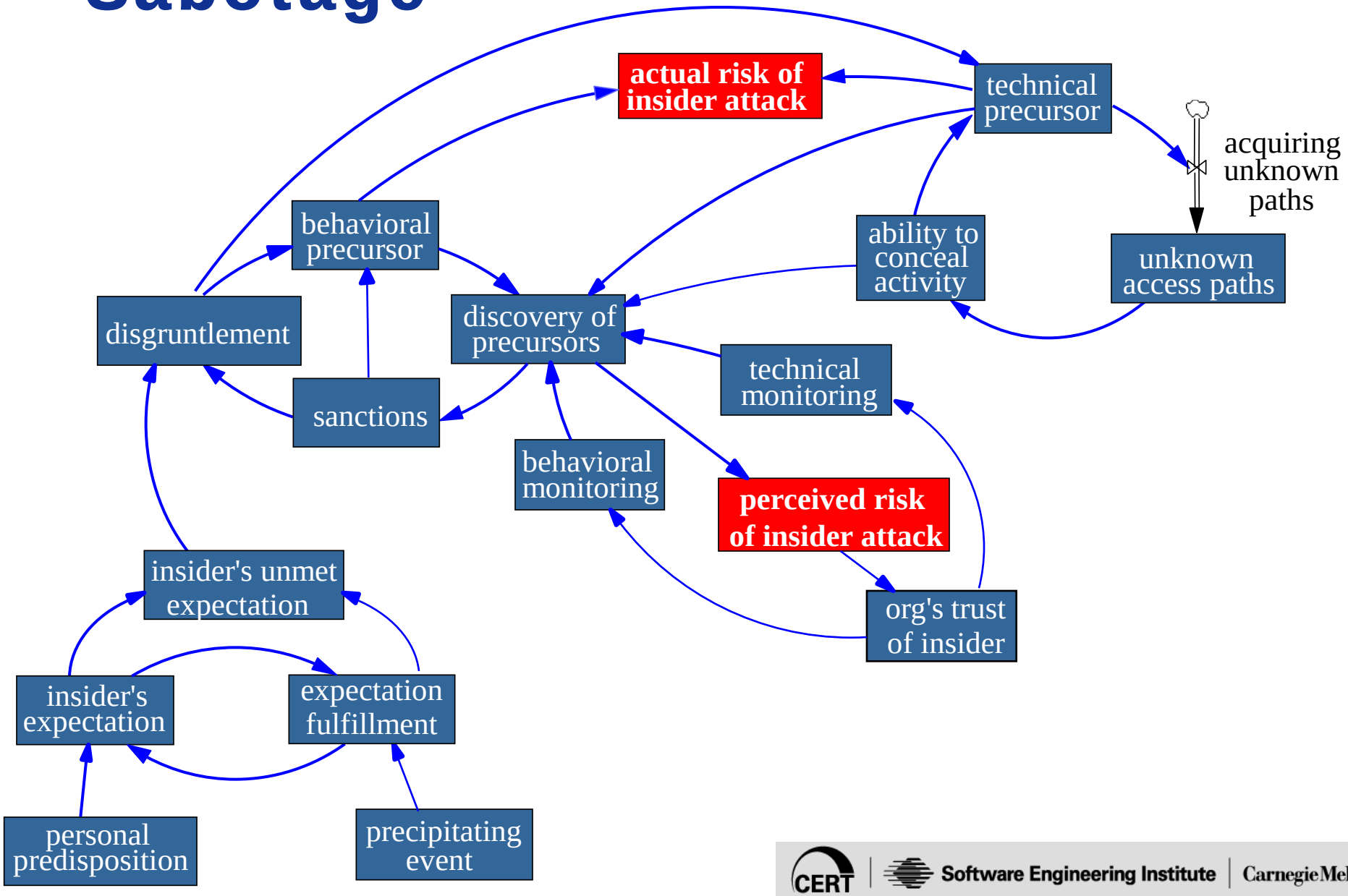
Summary of Findings – IT Sabotage

Current or former employee?	*Former*
Type of position	*Technical (e.g., system or database admins)*
Gender	*Primarily male*
Target	*Network, systems, or data*
Access used	*Unauthorized*
When	*Outside normal working hours*
Where	*Remote access*
Recruited by outsiders	*None*
Collusion	*None*

MERIT Model of Insider IT Sabotage



MERIT Model of Insider IT Sabotage



Countermeasures: Insider IT Sabotage

Strategy for Prevention of Insider IT Sabotage

- Need to prevent creation of unknown access paths
- Sample unknown access paths in the cases:
  - Planted logic bombs
  - Created backdoor accounts
  - Downloaded and installed malicious code or “hacker tools” such as rootkits, password sniffers, password crackers , viruses, …
  - Installed remote administration tool
  - Modified logs to conceal malicious activity
  - Disabled anti-virus and planted virus
- Why is prevention so difficult?
  - Privileged users have the ability to override system controls without detection
  - Information overload: can’t realistically monitor everything everyone does online

Solution Strategies

- Implement continuous logging and centralized, secure log server.
- Detect and investigate changes that should occur infrequently, such as:
  - Changes to operating system files, scripts, and executables
  - Changes to stable production systems
  - Services killed on host
- Audit individual actions in logs for privileged accounts.
  - Especially for insiders who are “on the HR radar”

Targeted Monitoring

Audit access to backup information and the results of backup and recovery tests carefully. **This is your last line of defense!**

Demos

Demo #2: Logic Bomb

Demo #3: Keylogger

Application to Your Organization

- In the first three months following this presentation you should:
  - Create policies and processes for proactive monitoring of employees with privileged access who are “on the HR radar”
  - Create an incident handling plan for detection and response to services killed on hosts, suspicious changes to operating system files, and modifications to stable production systems
- Within six months you should:
  - Implement and consistently enforce employee monitoring processes defined above
  - Implement incident handling plan for detection and response to services killed on hosts, suspicious changes to operating system files, and modifications to stable production systems
- ***This is a good place to start – stay tuned for what to do next!***

Caveats

- We only have data on criminals
  - Our findings/recommendations could result in a high false-positive rate.
  - We would like to work with organizations that are willing to be pilot sites. Please contact us.
- Monitoring techniques are not a guarantee.
  - In the event of a missed insider attack, these methods will be tremendously beneficial for incident response and forensic analysis teams.
- Consider legal, privacy, and policy issues before implementing any employee-monitoring program.

Food for Thought

- Which of the monitoring techniques we present today might also be effective in detecting external intruders if they manage to gain access?
- Could controls be effective against both insiders and outsiders?

Points of Contact

Technical Manager
CERT Insider Threat Center
Dawn M. Cappelli
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-9136 – Phone
dmc@cert.org – Email

Team Lead, Insider Threat Technical Solutions & Standards
Joji Montelibano
CERT Insider Threat Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
+1 412 268-6946 – Phone
jmm137@cert.org – Email

http://www.cert.org/insider_threat/